1088-12-269 **Nelly Fazio** and **Rosario Gennaro*** (rosario@cs.ccny.cuny.eduy), Center for Algorithms and Interactive, Scientific Software – CCNY, 160 Convent Ave – NAC 8/209, New York, NY 10031, and **Milinda Pereira** and **William E. Skeith**. *Diffie-Hellman Problems with Deterministic Hard-Core Bits.*

One of the long-standing open problems in cryptography is the security of individual bits of the secret value that results from a Diffie-Hellman key exchange. As of today no deterministic predicate of this secret value can be proven to be unpredictable. In this paper, we focus on the Diffie-Hellman problem over two specific platform groups: the group of points over elliptic curves and the multiplicative group of the quadratic extensions field over Fp. We solve this question by showing the first deterministic hard-core predicates for the Diffie-Hellman problem over those groups. Extending the Fourier-analysis and list decoding techniques by Akavia et al. and Duc et al. we show that under the assumption that computing the secret Diffie-Hellman value is hard in these group, then any individual bit of such secret value is unpredictable. (Received February 12, 2013)